Available online at www.sciencedirect.com

ScienceDirect

Procedia Economics and Finance 8 (2014) 336 – 345

Procedia Economics and Finance

www.elsevier.com/locate/procedia

1st International Conference 'Economic Scientific Research - Theoretical, Empirical and Practical Approaches', ESPERA 2013

Socio-economic major risks related to the information technology

Viorel Gaftea[a]*

"CERT-RO,B-dul. Maresal Averescu nr. 8-10, Etaj 1, Sector 1, Bucharest, Romania"

Abstract

Economy underwent a strong transformation in the last decade. Computerization, cybernetics, industrial robotics, communication and management are activities depending by IT.Society is knowledge based on IT and depending by online. Threats in the online reaches fever. Targets are critical infrastructure, telecommunications, energy, health, government and banking systems. Now there are on the pressure of cyber-attacks by multiple entities. Hackers evolve from "classic" e-mail infiltration or break websites of governmental institutions, to the cyber war as one of the newest and irregular forms of modern conflicts. The Risks are major and affect at nationally level and require preventive actions.Research is directed towards technology development, high level of computer usage and modern solutions for information management, risk control and total computerization of all activities.
In social, educationalarea the man isin user position, as target or initiator ofthe own actions but sometimes author of the risk generating actions.IT these generates major risks and required standards, policies, procedures and risk protection, "*instruments for systems in public and privatearea and for communicationequipment's using IT*".
Todayeconomy is based on all these elements and the evaluation of major risks related to the information technology become main priority.

*Keywords:*cyber security, national impact, major risks;

1. Major risk assumptions

Face to the problem of major risks phenomenon with impact at national level, firs of all we need to define them

* Corresponding author. Tel.: +4031-6202187; fax+4031-6202190.
*E-mail address:*viorel.gaftea@cert-ro.eu

doi:10.1016/S2212-5671(14)00099-9

in risk produced by:
-natural disasters like earthquakes, floods;
-human errors or destructive activities;
-economic disasters, produced by socio-human or financial factors;
-technical disasters like in hydro or nuclear energy systems;

What these situations have in common regarding a major risks? Information as data, statistics,communications, information technology monitoring infrastructure, theInternet.

2. Main risks points related to the information technology

Information security become today an Interdisciplinary activity to prevent major risks phenomenon with impact at national level. Targets are the critical infrastructure, telecommunications systems, computer systems, financial and banking systems, public administration, health or education systems.

Largest impact in today's society it is the information technology, the Internet.

For this reason the global organization is already known CERT (Computer Emergency Response Team) which has a subsidiary in Romania CERT-Ro (www.cert-ro.eu). ENISA (European Union Agency for Network and Information Security - www.enisa.europa.eu) is one of the most professional EU agencies whose research reports and policy underlying profile at both continental and national.

Reports published by CERT-Ro on security incidents allow us some analysis of the phenomenon in its depth. Technical capabilities of CERT-Ro relative to the realities of cyber security are an important step in the adoption of the EU Directive on Information Security and Networks (Network and Information Security -NIS).

Based upon the data collected by CERT_RO (the 2013 report) were observedthe phenomena at a national level regarding the Internet major's risks:

- riskssuch in computer science, the national cyberspace have diversified,
-12.5% of beach-IPs allocated to Romania is infected with various malware variants
-5678 domanins**".ro"**were compromised, this representing less than 1% of existing domains.

The Levels of exposure to main risks related to Internet,refer generally the connection to public and free /unprotected networks determine the level of risk:

- Free conection (direct connection in Internet network)
- Firewall (address screening/ network isolation)
- DMZ (use DNS Server)
- No connection (internal network /Intranet
- The complexsolution can contain combination over the base structure presented.
- What these situations have in common regarding the major risks protection? First of all: Alerts !
- Major Risks imposes as first measure to have an alert systems. How can be treated Internet alerts?

There are generated by:

- Anonymous: contributions send it by known or unknowns users;
- Official: alerts send it by public or professional organizations like CERT, Emergency systems or trough institutional websites.

3. CERT-RO Research report

First CERT (www.cert.org) was created by DARPA (Defense Advanced Research Projects Agency) in 1988 to deal with internet security problems after the Morris Worm struck. Its coordination centre (CERT/CC) is located at CarnegieMellonUniversity's Software Engineering Institute (SEI - http://www.cmu.edu). The Morris Worm had widespread repercussions and infected thousands of machines. SEI CERT/CC was established to deal with internet security and, for 12 to 15 years, studied cases of software vulnerabilities and compiled a database of them. The Secure Coding Initiative, launched in 2005, used this database to help develop secure coding practices.

Table 1.Type of main Internet alerts

Clasa alerte	Tip Alertă	Număr alerte	IP-uri unice
Botnet	Botnet drone	15.577.697	1.546.472
Spam	Spam	1.797.158	456.270
Malware infected resource	Malicious URL	46.332	2.258
Scanners	Scanners	39.732	3.627
Open resources	Openresolver	33.165	28.035
Intrusion attempts	Bruteforce	8.439	47
Open resources	Open-proxy	4.931	191
Malware infected resource	Infected machine	1.704	264
Phishing	Phishing URL	1.669	276
Botnet	Botnet C&C	282	85
TOTAL		**17.511.109**	**2.037.525**

Tabel 1 – Repartiția alertelor pe tipuri de incidente

From Romanian CERT-RO research activities report we present in adjacent tables thetype of alerts received, class distribution and types of alerts in Internet space. Some IP –internet addresses are unique and can be found reported in several categories of alerts.

3.1 The geographical distribution of IPs reported

For over 1,454,935 of reported IPs were identified on the basis of geographical location geo-location service offered by MaxMind3. Thus, the distribution table retrieves IP addresses reported by region or cities in Romania. From localities reported, we present Top 10.

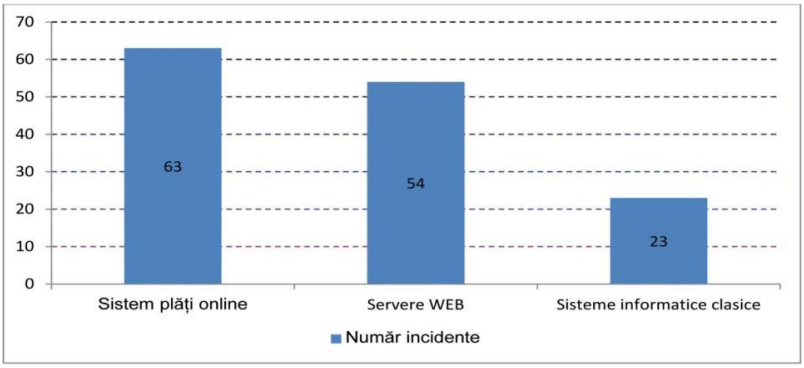
Table 2. The geographical distribution of IPs

Nr. Crt.	Oraș/Regiune	Nr. IP-uri	Nr. Crt.	Oraș/Regiune	Nr. IP-uri	Nr. Crt.	Oraș/Regiune	Nr. IP-uri	Nr. Crt.	Oraș/Regiune	Nr. IP-uri
1	Bucuresti	288.366	51	Brebu	2.932	101	Ianca	709	151	Filipestii De Padure	107
2	Neidentificat	189.720	52	Pascani	2.704	102	Tecuci	704	152	Joseni	105
3	Iasi	62.274	53	Husi	2.665	103	Carei	676	153	Jilava	100
4	Constanta	59.227	54	Pantelimon	2.567	104	Dragasani	675	154	Lipanesti	92
5	Oradea	55.454	55	Turnu Magurele	2.472	105	Chiajna	665	155	Rosiorii De Vede	88
6	Timisoara	53.410	56	Otopeni	2.452	106	Moldova Noua	631	156	Barcanesti	86
7	Craiova	50.298	57	Gherla	2.428	107	Uricani	587	157	Buzias	79
8	Galati	46.912	58	Motru	2.293	108	Busteni	571	158	Moldovita	79
9	Brasov	46.135	59	Cernavoda	2.202	109	Orsova	542	159	Miercurea	69
10	Cluj-napoca	42.481	60	Fagaras	2.170	110	Buftea	540	160	Berceni	63

3.2 .Distributionof "incidentsper affected entities"

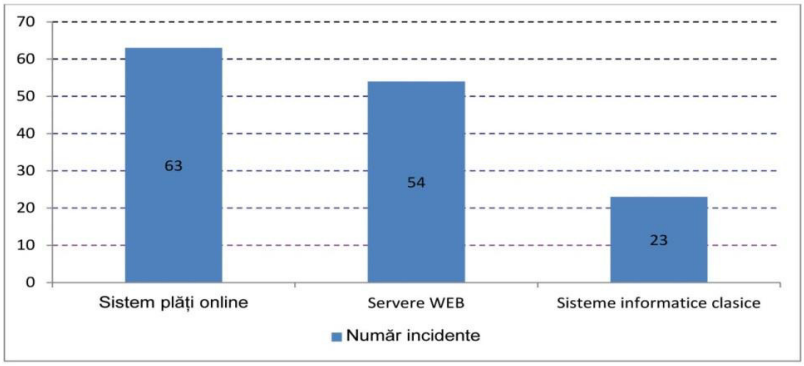
The Depending on the incident distribution in affected entities is presented in the chart below. It is worth mentioning that the entities affected are not necessarily natural or legal persons in Romania and refer in order in next figure to "*banks, firms, individuals, public institution and education*".

Table 3. The number of incidents per affected entities



Also, depending on the type of affect, the distribution of security incidents are distributed as follows:„highest in online payment systems, web servers and informatic systems".

Table 4. The number of incidents per services



4. "Major Risks View face to the Information Technology"

Firstshall specify thesocio-economic andriskimplications ofmajordirectionsin which theycan act.The world now is in a continue motion. Steps from ‘’vulnerability’’ to ‘’action’’ are presented in the general context in the next figure.

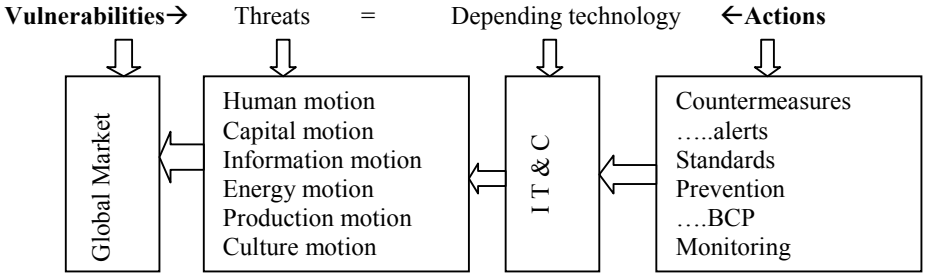


Figure 1.Dependence chain from IT

Determining the points of failure, point of monitoring, point of intervention are the most important.

How adapt and protect national systems in a responsiblemode ?

Is enough the management of information systems or are necessary auxiliary actions?

In the figure 1 the equilibrium is made by ‘’Vulnerability= Action’’ *(trough IT Technologies used to respond to Threats*).

The European Commission recognizes the need for developing standards in the new technological environment like ‘’cloud domain’’, and has worked closely with ETSI to map existing standards and explore potential gaps, a single market for cloud computing, adopted as European project.

In the world are diversified solutions adopted, “Vulnerability information and mitigations for software products”refers to traffic monitoring systems that observes the Internet threats,enabling the development of countermeasures.

Must in this point to define the new global context as Digital Space.First paradigm Digital Life versus Digital Firm must now completed by Digital Environment.In this working Virtual Space must define: “ whoreglement, who control, whomonitorize this space”.

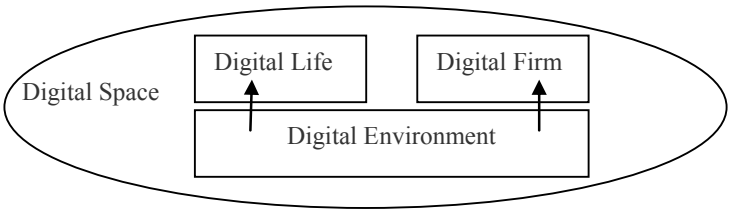


Fig.2.Digital Space

The common element of new approach is DATA. Data can be in context with:

- Data access ←→ how quickly
- Data consistency ←→ how integrity
- Data continuity ←→ how secure

All criteria are applied to ‘*’production, energy, education, finance, education systems and governmental or private sectors*’’.

The major questions and response are:

-	What are their *common* major risks factors?	IT?
-	Who determinesthem?	Human and Technical factors
-	How can we prevent?	Prevent, Alerts and Monitoring

- Who is responsible?Is Individual or Institutional duty?

Institutional, the legal frame regarding IT services is running in Romania. We mention:

- Services of electronic certificates - Law 455/2001 on electronic signature
- Services of temporary marking - Law 451/2004 on temporal marking,
- Services of electronic archiving with legal value - Law 135/2007 on archiving documents in electronic form
- Services of electronic invoicing - Law 148/2012 on invoice in electronic form.

5. "Major Risks View face to the national economy"

Two problems may face to analysis of major risks determinated by IT in economy:

a) The impact of IT sectors in the economy
b) What is IT impact into the whole economy
c) What is the cost of inaction or delayed action against major risks?

a)-The common impact of IT sectors in the economy do not exceed 5-6%

The results of IT impact studiesshow that, the USinformation sector grew at a slightly quickly rate than did the entireeconomy.

Romanian analysis reflect a smaller impact of IT sector in economy. Rhetoric question is: *Mean these smaller risks*? Next statistics suggest us a medium impact but very important for the few players in IT.

Table 5.IT indicators specific to Romanian economy

Indicators	2010	2011
Number of enterprises	15,570	14,595
Average number of employees (thousands individuals)	121,000	128,000
Turnover of enterprises (mil. lei)	40,474	40,113
Staff costs (mil. lei)	5,865	6,671
Gross added value (mil. lei)	14,107	14,320
Gross operation excess (mil.lei)	8,243	5,236
Investments performed (mil. lei)	2,600	3,016
Share of turnover of enterprises in the TIC field of the overall turnover of enterprises with economic activity (%)	4.6%	4.1%
Share of turnover of enterprises with main activity of editing software products and service activities in information technology overall the turnover of enterprises with IT main activity (%)	23.2%	24.8%
Share of the turnover of enterprises with main activity of telecommunication overall the turnover of enterprises with IT main activity (%)	43.7%	47.2%
Turnover of the activity of editing software products and service activities in technology of information (mil. lei)	9,408	9,959

Source: INS, National Institute for Statistics, 2013[†]

b)-IT impact into the whole economy is around 5-6%

Table 6.Situation of sub-sector of Information and Communication, 2009

	Turnover (mil. RON)	Export (mil. RON)	Import (mil. RON)
Total Information and Communications, out of which:	35,032.86	14,085.90	16,666.20
Hardware	8,502.30	8,671.50	13,536.00
Software and IT services	8,066.61	2,622.60	1,353.60

[†]http://www.insse.ro/cms/files/ISI/publicatia_SI_13.pdf

Telecom services	18,463.95	2,791.80	1,776.60

Source: MECMA, National Strategy of Export of Romania, 2011-2015[‡]

The functionality of main informatics platform which provides services to the citizens can be considered as major risk at national level? No, because no interoperability between actual Electronic Public Systems.The low dependency of governmental functionality by the continuity of this IT public services contrast with banking and stock-market networks and Communications, represented by fixed and mobile operators were risk management and disaster recovery procedures works.

c)-Riskassociated witheach specificIT productenablescost-likelihood estimationwitha table ofvulnerabilities where human interactionoccursas a main factor ofvulnerability, a decisive one.

To estimate the impact cost we present the analysis in next figure:

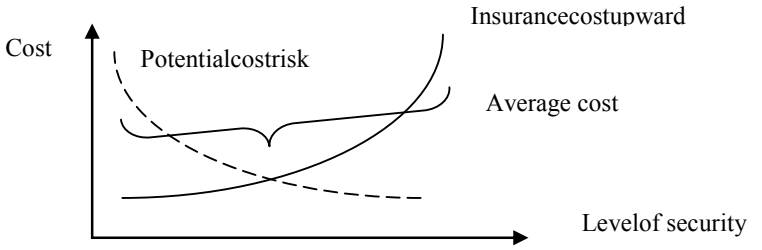


Fig.3.Cost of security measures

Average costassociated(in accolade representation) is affected by the costof retribution of humanfactor as first vulnerability according to most recent studies.Cost of security measuresmust not exceed the investment; ISO27001, Cobittstandards, etc. give us the correct estimation rules and measures that must put in place.

5.1 Estimation methods

In previous researches like Zipf's law,researcher define that an event size depends on the rank-correlation, extrapolatingto the size www 'world wide web', can determine the impact inGDP.

Major RiskSize = Konstant * Ranking Risk atPower –p,

where-p =-0.93, was theoretically/experimentally determined but need more simulation for our economy.

The problem is treated at global level, by specialized organization, (http://thewebindex.org/), the World Bank result study (https://beta.thewebindex.org/wp-content/uploads/2013/11/Web-Index-Annual-Report-2013-FINAL.pdf) presents GDP per capita in PPP$ – VS. WEB INDEX SCORE.

The impact related to main economic macro indicator GDP, on a graphic representation "GDP / number of sites" can approximate the evolution and the impact, indirect associated risks in same time.

An association:

-ona scale from 4 to1 (Free connection, Firewall, DMZ, No connection),

- ona second scale from 4 to 1 (national, regional, county, community), permit us to simulate the power of an event associated to a major risk in a national area. Detailed information and exact determinations must completed by a research and statistical data, we suggest here only an analysis way.

[‡] http://www.minind.ro/propuneri_legislative/2011/mai/SNE_2011_2015.pdf

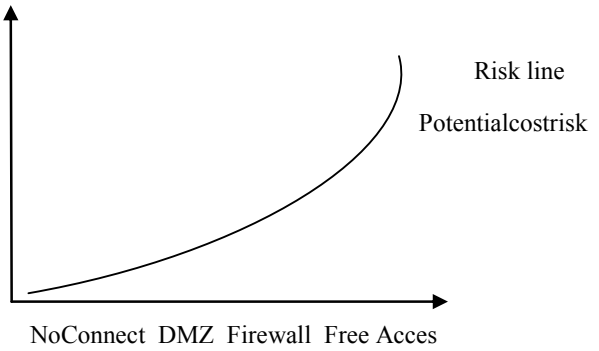


Figure4.Risk line associated to system vulnerability and wide spread

The graphic represents simultaneous multiple correlations between level of vulnerabilities and level o risks and associated costs.

The Depending from Interdisciplinary programs to prevent major risks phenomenon at national level,imposes assessment phases in all sectors, projects that must contain risk management from first to last:

1. Design requirements
2. The design himself
3. The Development and The Tests
4. Production
5. Monitoring, which often is not taken into account?

Conclusion

Threats, such in computer science, in the national cyberspace are more diversified by revolutionary trends, both highlighted quantitatively increasein terms of technical complexity and as number.

In future, in the category of critical systems, IT&C must be included and two action must be planed:

- Increasing security, as response to;
- Increasing number of attacks.

Which willbe more effective? Response: **The chain "education, prevention, monitoring and alerts".**

The chain must be completed by functionality in a '**reglemented cadre, standards and procedures**'.

The subject is very actually and generalized.

The European Commission informed about the timetable for structural funds in the new programming period 2014-2020 and invited members to prioritize ICT funding in their strategic Partnership Agreements and Operational Programmes.

Focus will be on the following topics:

- The ‘’Connected Continent’' package
- Taxation and OTT-players, re-considering position on tax breaks for R&D&I investments
- Internet governance.

These increase exposure to major risks depending by IT.

The upcoming Greek Presidency of the EU has already indicated NIS as a priority dossier and will strive to achieve adoption by the end of the legislature. The Commission provided an overview of the state of play of the NIS Directive and the EU Cyber security strategy.

In this point we must to specify the top 10 area of direct risk in IT, very easy to transform in major risks:

1. Social Networking - Unauthorized access to confidential data,
2. Mobile Devices - Security and identity management,
3. Malware - Loss or theft of critical information,
4. End User Computing -Loss or corruption of data,
5. Corporate Espionage- Loss or release of corporate data/ Denial of service,
6. Project Backlog (delays, failure),
7. IT Governance -Information security risks/ duplication efforts, increased costs, inefficiencies,
8. Electronic Records Management (ERM) loss of data, violation, storage,
9. Data Management -Increased cost of compliance,
10. Cloud Computing -location/compliance/recovery/security/Investigative support.

The Global Risks Report 2013 analyses 50 global risks in terms of impact, cyber attacks are in Technological analysis in a top position. http://www.weforum.org/reports/global-risks-2013-eighth-edition, (http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2013.pdf).

Acknowledgements

Acknowledgements to CERT-ROTeam (www.cert-ro.eu) and their activity, to General Directors; LiviuNicolescu and Eduard Bisceanu.

Appendix A. Romanian regulatory framework regarding the cybernetic security aspects

1. The protection of the users’ data

a) Law no. 677/2001 on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of Such Data, amended and completed.

b) Law no. 506/2004 on the processing of personal data and the protection of privacy in the electronic communications sector.

c) Ministry Order no. 389/2007 on the procedure for approval of payment instruments with remote access applications such as Internet banking, home-banking or mobile banking.

2. **The prevention and the suppression of the cybercrime**

a) Law no. 161/2003, title III, regarding the Prevention and Suppression of the Cybercrime, subsequently amended and supplemented.

b) Law no. 365/2002 on electronic commerce.

c) Government Decision no. 494/2011 establishing the role of CERT-RO.

d) Law no. 82/2012 regarding the retention of general data or data processed by the electronic communications public networks providers and electronic communications for public use providers, as well as for the modification and completion of the Law no. 506/2004 on the processing of personal data and the protection of privacy in the electronic communications sector.

3. **Mechanisms for the provision of data protection**

a) Law no. 455/2001 on the electronic signature.

b) Law no. 451/2004 on time stamping.

c) Law no. 589/2004 on the legal status of electronic notarial activity.
d) Law no. 135/2007 on the archiving of documents in electronic form.
e) Law no. 148/2012 which establishes the legal framework for the issuing of electronic documents.
f) Governmental Decision no. 962/2010 for the approval of the technique of developing the national system for national social health insurance cards.
Emergency Government Ordinance no. 124/2010 on the modification of the Government Ordinance no. 69/2002 on the legal regime of the identity electronic card.

References

Analysis report on 2013, CERT-RO, http://www.cert-ro.eu/articol.php?idarticol=755,
http://www.cert-ro.eu/files/doc/755_20130829160854010360100_X.pdf
Digital Agenda, 2013, Ministry for Information Society
Filip, F.G,Simionescu, B. 2004, Fenomenesiprocese cu risc major la scaranationala, EdituraAcademieiRomane, ISBN 973-27-1150-7
Filip, F.G., 2001, SocietateaInformationala, Societateacunoasterii,EdituraExpertAcademieiRomane, ISBN 973-8177-42-1
Japan CERT, 2013, http://www.jpcert.or.jp/english/
National Computer Security Incident Response Teams, http://www.cert.org/csirts/national/contact.html
Michael Rogers Rubin And ElizabethTaylor,. 1981, The U.S. Information Sector And GNP:An Input-Output Study, Informotion Processing & Management. Vol. 17. Pp. 163.194
Schiode, N. Power Inet 2000, Law Disribution in Real and Virtual Worlds, Procedingswww.isoc.org/inet2000.